Nasihat APT40

PRC MSS kemahiran spionase tengah beraksi

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

Daftar isi

Ikhtisar

Latar Belakang

Nasihat ini, yang ditulis oleh Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), United States Cybersecurity and Infrastructure Security Agency (CISA), United States National Security Agency (NSA), United States Federal Bureau of Investigation (FBI), United Kingdom National Cyber Security Centre (NCSC-UK), Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NCSC-NZ), German Federal Intelligence Service (BND) dan Federal Office for the Protection of the Constitution (BfV), Republic of Korea's National Intelligence Service (NIS) dan NIS National Cyber Security Center, dan National Center of Incident Readiness and Strategy for Cybersecurity (NISC) dan National Police Agency (NPA) Jepang – selanjutnya disebut sebagai "badan penyusun" – menguraikan kelompok siber yang disponsori negara Republik Rakyat Tiongkok (RRT) dan ancaman mereka saat ini terhadap jaringan Australia. Nasihat ini mengacu kepada pemahaman bersama dari badan penyusun mengenai ancaman tersebut serta investigasi respons insiden ACSC ASD.

Kelompok siber yang disponsori negara RRT sebelumnya telah menargetkan organisasi di berbagai negara, termasuk Australia dan Amerika Serikat, dan teknik yang disorot di bawah ini secara teratur digunakan oleh pelaku lain yang disponsori negara RRT di seluruh dunia. Oleh karena itu, lembaga-lembaga pembuatnya meyakini bahwa kelompok tersebut dan teknik-teknik serupa tetap menjadi ancaman bagi jaringan negara mereka.

Badan penyusun menilai bahwa kelompok ini melakukan operasi kejahatan ciber untuk Kementerian Keamanan Negara RRT (MSS). Aktivitas dan tekniknya tumpang tindih dengan kelompok yang dilacak sebagai Advanced Persistent Threat (APT) 40 (juga dikenal sebagai Kryptonite Panda, GINGHAM TYPHOON, Leviathan, dan Bronze Mohawk dalam pelaporan industri). Kelompok ini sebelumnya dilaporkan bermarkas di Haikou, Provinsi Hainan, RRT, dan menerima penugasan dari MSS RRT, Departemen Keamanan Negara Hainan.[2] Nasihat berikut memberikan contoh studi kasus penting tentang teknik penyerang ini dalam aksinya terhadap dua jaringan korban. Studi kasus ini penting bagi praktisi keamanan siber untuk mengidentifikasi, mencegah, dan memulihkan intrusi APT40 terhadap jaringan mereka sendiri. Studi kasus yang dipilih adalah studi kasus yang telah dilakukan pemulihan yang tepat untuk mengurangi risiko eksploitasi ulang oleh pelaku ancaman ini, atau yang lainnya. Oleh karena itu, studi kasus ini umumnya sudah lama, untuk memastikan organisasi diberi waktu yang diperlukan untuk memulihkan.

Ringkasan Aktivitas

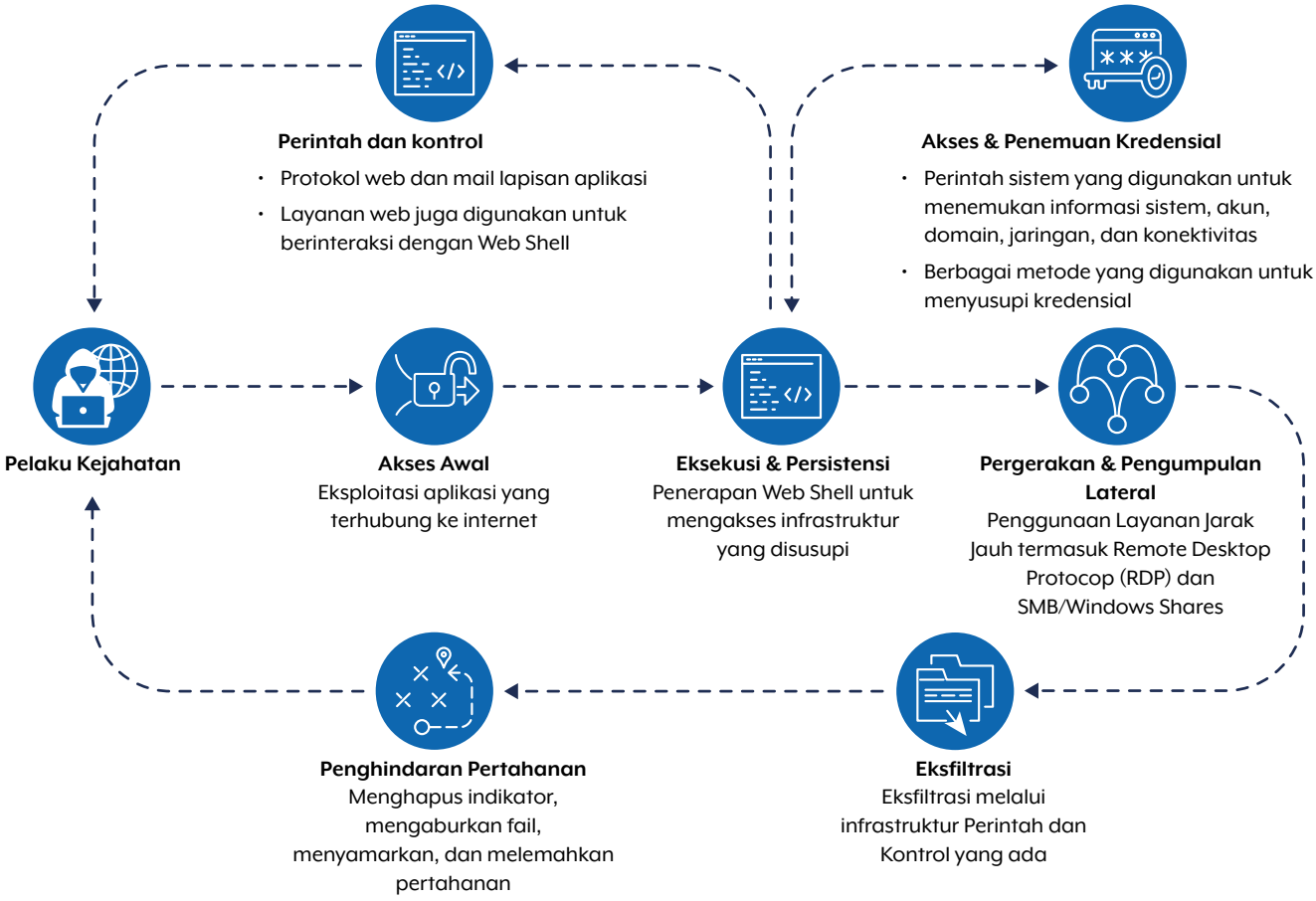
APT40 telah berulang kali menargetkan jaringan Australia serta jaringan pemerintah dan sektor swasta di kawasan tersebut, dan ancaman yang mereka timbulkan terhadap jaringan kami masih berlangsung. Kemahiran spionase yang dijelaskan dalam nasihat ini secara berkala diamati terhadap jaringan Australia.

Terutama, APT40 memiliki kemampuan untuk dengan cepat mentransformasi dan mengadaptasi bukti konsep (POC) eksploitasi kerentanan baru dan segera memanfaatkannya terhadap jaringan target yang memiliki infrastruktur kerentanan terkait. APT40 secara berkala melakukan pengintaian terhadap jaringan yang dimaksud, termasuk jaringan di negara-negara badan penyusun, untuk mencari peluang untuk mengotak-atik targetnya. Pengintaian berkala ini memposisikan kelompok tersebut untuk mengidentifikasi perangkat yang rentan, yang sudah habis masa pakainya, atau tidak lagi dipelihara pada jaringan yang dimaksud, dan untuk segera menyebarkan eksploitasi. APT40 terus menemukan keberhasilan dalam mengeksploitasi kerentanan sejak tahun 2017.

APT40 dengan cepat mengeksploitasi kerentanan publik baru dalam perangkat lunak yang banyak digunakan seperti Log4J (CVE 2021 44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) dan Microsoft Exchange (CVE-2021-31207; CVE-2021-34523; CVE-2021-34473). ACSC ASD dan badan penyusun memperkirakan kelompok tersebut akan terus menggunakan POC untuk kerentanan baru yang berisiko tinggi dalam hitungan jam atau hari setelah rilis ke publik.

2 Departemen Kehakiman AS. 2021. Empat Warga Negara Tiongkok yang Bekerja dengan Kementerian Keamanan Negara Didakwa atas Kampanye Intrusi Komputer Global yang Menargetkan Kekayaan Intelektual dan Informasi Bisnis Rahasia, Termasuk Penelitian Penyakit Menular.

Gambar 1. Diagram alir TTP untuk aktivitas APT40



Kelompok ini tampaknya lebih memilih mengeksploitasi infrastruktur publik yang rentan daripada teknik yang memerlukan interaksi pengguna, seperti kampanye phishing, dan menempatkan prioritas tinggi pada perolehan kredensial yang valid untuk memungkinkan serangkaian aktivitas lanjutan. APT40 secara teratur menggunakan web shell (T1505.003) untuk persistensi, terutama di awal siklus hidup intrusi. Biasanya, setelah akses awal berhasil, APT40 berfokus pada pembentukan persistensi untuk mempertahankan akses pada lingkungan korban. Namun, karena persistensi terjadi pada awal intrusi, persistensi lebih mungkin diamati pada semua intrusi – terlepas dari tingkat penyusupan atau tindakan lebih lanjut yang diambil.

Kemahiran Spionase yang Terkenal

Meskipun APT40 sebelumnya menggunakan situs web Australia yang disusupi sebagai host perintah dan kontrol (C2) untuk operasinya, kelompok tersebut telah mengembangkan teknik tersebut (T1594).

APT40 telah mengadopsi tren global penggunaan perangkat yang telah disusupi, termasuk perangkat small-office/home-office (SOHO), sebagai infrastruktur operasional dan pengalihan lompatan terakhir (T1584.008) untuk operasinya di Australia. Hal ini memungkinkan badan penyusun untuk menggambarkan karakterisasi dan melacak pergerakan kelompok ini dengan lebih baik.

Banyak perangkat SOHO ini sudah habis masa pakainya atau belum diperbaiki dan menjadi target empuk untuk eksploitasi N-day. Setelah disusupi, perangkat SOHO menjadi titik awal serangan yang dirancang untuk berbaur dengan lalu lintas yang sah dan menantang pertahanan jaringan (T1001.003).

Teknik ini juga secara rutin digunakan oleh pelaku-pelaku lain yang disponsori negara RRT di seluruh dunia, dan badan penyusun menganggap hal ini sebagai ancaman bersama. Untuk informasi tambahan, lihat nasihat bersama Pelaku Siber yang Disponsori Negara Republik Rakyat Tiongkok Memanfaatkan Penyedia Jaringan dan Perangkat dan Pelaku yang Disponsori Negara RRT Mengkompromikan dan Mempertahankan Akses Berkelanjutan ke Infrastruktur Kritis AS.

APT40 kadang-kadang menggunakan infrastruktur yang diperoleh atau disewa sebagai infrastruktur C2 yang berhadapan dengan korban dalam operasinya; namun, kemahiran spionase ini tampaknya mengalami penurunan relatif.

Peralatan

ACSC ASD membagikan beberapa fail berbahaya yang teridentifikasi selama investigasi yang diuraikan di bawah ini. Fail-fail ini telah diunggah ke VirusTotal untuk memungkinkan komunitas pertahanan jaringan dan keamanan siber yang lebih luas guna lebih memahami ancaman yang perlu mereka lawan.

Studi Kasus

ACSC ASD membagikan dua laporan investigasi anonim untuk memberikan kesadaran tentang bagaimana para pelaku menggunakan alat dan kemahiran spionase mereka

MD5	Nama Fail	Informasi tambahan
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Java Source
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Java Bytecode
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Java Bytecode
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Java Source
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Java Bytecode
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Java Bytecode
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Java Bytecode
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Java Bytecode
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Java Bytecode
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Java Source

Studi Kasus 1

Laporan ini telah dianonimkan agar dapat disebarluaskan kepada publik. Organisasi yang terdampak selanjutnya disebut sebagai 'organisasi'. Beberapa detail spesifik telah dihapus untuk melindungi identitas korban dan metode respons insiden ACSC ASD.

Ringkasan Eksekutif

Laporan ini memerinci temuan investigasi ACSC ASD terhadap keberhasilan penyusupan jaringan organisasi antara Juli dan September 2022. Laporan investigasi ini diberikan kepada organisasi untuk merangkum aktivitas kejahatan yang teramati dan menyusun rekomendasi remediasi. Temuan menunjukkan bahwa pembobolan dilakukan oleh APT40.

Pada pertengahan Agustus, ACSC ASD memberi tahu organisasi tersebut tentang interaksi kejahatan dengan jaringan mereka dari perangkat yang kemungkinan telah disusupi yang digunakan oleh grup tersebut pada akhir Agustus dan, dengan persetujuan organisasi, ACSC ASD menerapkan sensor berbasis host ke host yang kemungkinan terdampak di jaringan organisasi. Sensor-sensor ini memungkinkan analis respons insiden ACSC ASD untuk melakukan investigasi forensik digital yang menyeluruh. Dengan menggunakan data sensor yang tersedia, analis ACSC ASD berhasil memetakan aktivitas grup dan membuat linimasa terperinci dari peristiwa yang teramati.

Dari Juli hingga Agustus, aktivitas pelaku kunci yang diamati oleh ACSC ASD meliputi:

- enumerasi host, yang memungkinkan pelaku membangun peta jaringannya sendiri;
- penggunaan web shell, yang memberi pelaku pijakan awal di jaringan dan kemampuan untuk menjalankan perintah; dan
- penyebaran peralatan lain yang dimanfaatkan oleh pelaku untuk tujuan kejahatan.

Investigasi ini mengungkap bukti adanya akses terhadap sejumlah besar data sensitif dan bukti bahwa para pelaku bergerak secara lateral melalui jaringan (T1021.002). Sebagian besar penyusupan difasilitasi oleh pembentukan beberapa vektor akses ke jaringan oleh kelompok tersebut, jaringan yang memiliki struktur datar, dan penggunaan perangkat lunak internal yang tidak aman yang dapat digunakan untuk mengunggah fail secara sembarangan. Data yang dieksfiltrasi mencakup kredensial autentikasi istimewa yang memungkinkan kelompok tersebut untuk masuk, serta informasi jaringan yang memungkinkan pelaku mendapatkan kembali akses tidak sah jika vektor akses asli diblokir. Tidak ditemukan peralatan berbahaya tambahan selain yang ada di mesin yang dieksploitasi pertama kali; namun, akses suatu kelompok ke kredensial yang sah dan istimewa akan meniadakan kebutuhan akan peralatan tambahan. Temuan investigasi menunjukkan organisasi tersebut kemungkinan besar sengaja ditargetkan oleh APT40, bukannya menjadi korban oportunistik dari kerentanan yang diketahui publik.

Penemuan investigasi

Pada pertengahan Agustus 2022, ACSC ASD memberi tahu organisasi tersebut bahwa IP berbahaya yang dikonfirmasi dan diyakini berafiliasi dengan kelompok siber yang disponsori negara telah berinteraksi dengan jaringan komputer organisasi tersebut setidaknya antara Juli dan Agustus. Perangkat yang disusupi kemungkinan besar milik pengguna bisnis kecil atau pengguna rumahan.

Pada akhir Agustus, ACSC ASD menyebarkan agen berbasis host ke host-host di jaringan organisasi yang menunjukkan bukti telah terdampak oleh penyusupan tersebut.

Beberapa artefak yang dapat mendukung upaya investigasi tidak tersedia karena konfigurasi logging atau desain jaringan. Meskipun demikian, kesiapan organisasi untuk menyediakan semua data yang ada memungkinkan responden insiden ACSC ASD untuk melakukan analisis komprehensif dan membentuk pemahaman tentang kemungkinan aktivitas APT40 di jaringan.

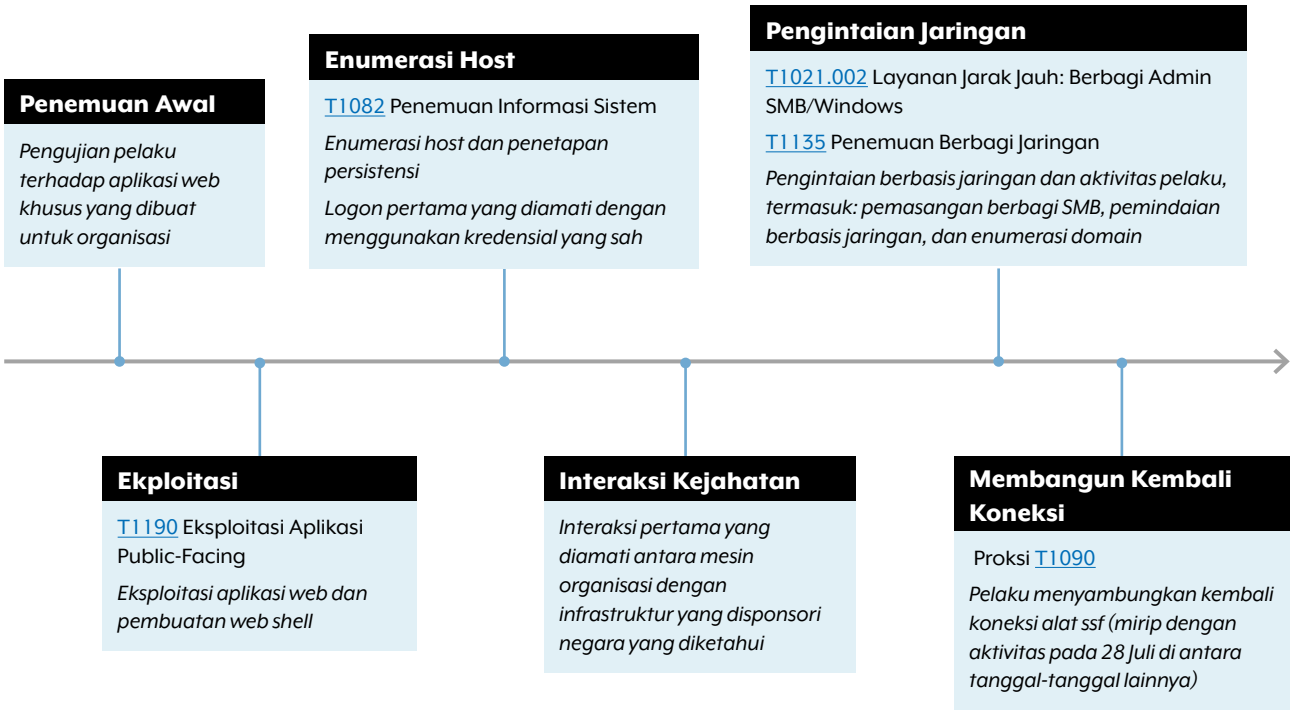
Pada bulan September, setelah berkonsultasi dengan ACSC ASD, organisasi tersebut memutuskan untuk menolak IP yang diidentifikasi dalam pemberitahuan awal. Pada bulan Oktober, organisasi tersebut memulai proses remediasi.

Detail

Dimulai pada bulan Juli, para pelaku dapat menguji dan mengeksploitasi aplikasi web khusus (T1190) yang berjalan pada `<webapp>2-ext`, yang memungkinkan kelompok tersebut untuk membangun pijakan di jaringan zona demiliterisasi (DMZ). Ini dimanfaatkan untuk menghitung jaringan dan semua domain yang terlihat. Kredensial yang disusupi (T1078.002) digunakan untuk menanyakan Direktori Aktif (T1018) dan mengeksfiltrasi data dengan memasang berbagi fail (T1039) dari beberapa mesin dalam DMZ. Pelaku tersebut melakukan serangan Kerberoasting untuk mendapatkan kredensial jaringan yang valid dari server (T1558.003). Kelompok tersebut tidak teramati memperoleh poin kehadiran tambahan baik di DMZ maupun jaringan internal.

Lini masa visual

Lini masa di bawah ini memberikan gambaran umum tentang fase-fase utama aktivitas pelaku kejahatan yang diamati pada jaringan organisasi.



Lini Masa Terperinci

Juli: Para pelaku membuat koneksi awal ke halaman depan aplikasi web khusus (T1190) yang dibuat untuk organisasi tersebut (selanjutnya disebut sebagai 'web application' or '*webapp*') melalui koneksi keamanan lapisan transport (TLS) (T1102). Tidak ada aktivitas penting lain yang teramati.

Juli: Para pelaku mulai menelusuri situs web application tersebut untuk mencari titik akhir[2] guna diselidiki lebih lanjut.

Juli: Para pelaku berkonsentrasi pada upaya untuk mengeksploitasi titik akhir tertentu.

Juli: Para pelaku berhasil `POST` ke server web, kemungkinan melalui web shell yang ditempatkan di halaman lain. IP kedua, yang kemungkinan digunakan oleh pelaku yang sama, juga mulai memposting ke URL yang sama. Para pelaku menciptakan dan menguji sejumlah kemungkinan web shell.

Metode eksploitasi yang tepat tidak diketahui, tetapi jelas bahwa titik akhir spesifik ditargetkan untuk membuat fail di `<webapp>2-ext`.

ACSC ASD meyakini bahwa dua koneksi alamat IP tersebut merupakan bagian dari intrusi yang sama karena memiliki kepentingan yang sama dan koneksi awal terjadi dengan selisih beberapa menit.

Juli: Kelompok ini terus melakukan enumerasi host, mencari peluang eskalasi hak istimewa, dan menerapkan web shell yang berbeda. Para pelaku masuk ke aplikasi web menggunakan kredensial yang disusupi untuk `<firstname.surname>@<organisation domain>`.

Aktivitas pelaku tampaknya tidak berhasil mencapai peningkatan hak istimewa pada `<webapp>2-ext`. Sebaliknya, para pelaku beralih ke aktivitas berbasis jaringan.

Juli: Pelaku menguji kredensial yang disusupi untuk akun layanan[3] yang kemungkinan ditemukan terkode keras dalam biner yang dapat diakses secara internal.

Juli: Para pelaku menggunakan alat sumber terbuka Secure Socket Funnelling, yang digunakan untuk terhubung ke infrastruktur berbahaya. Koneksi ini digunakan untuk menyalurkan lalu lintas dari mesin penyerang milik pelaku ke jaringan internal organisasi, yang nama mesinnya terekspos dalam log peristiwa saat mereka mencoba menggunakan kredensial untuk akun layanan.

Agustus: Para pelaku terlihat melakukan sejumlah aktivitas terbatas, termasuk gagal membuat koneksi yang melibatkan akun layanan.

Agustus: Para pelaku melakukan enumerasi jaringan dan Direktori Aktif yang signifikan. Akun lain yang disusupi kemudian digunakan untuk memasang share[4] pada mesin Windows di dalam DMZ, yang memungkinkan eksfiltrasi data yang berhasil.

Hal ini tampaknya merupakan penggunaan oportunistik dari kredensial yang dicuri pada mesin yang dapat dipasang di DMZ. Firewall memblokir pelaku tersebut agar tidak menargetkan jaringan internal dengan aktivitas serupa.

Agustus-September: Alat SSF berhasil memulihkan koneksi ke IP berbahaya. Kelompok tersebut tidak terlihat melakukan aktivitas tambahan apa pun hingga akses mereka diblokir.

September: Organisasi memblokir IP berbahaya dengan memasukkannya ke dalam daftar penolakan di firewall mereka.

2 Dalam konteks ini, titik akhir adalah fungsi dari aplikasi web.

3 Akun layanan tidak terikat dengan pengguna individu, melainkan dengan layanan. Dalam domain perusahaan Microsoft, terdapat berbagai jenis akun.

4 Memasang shares adalah proses membuat fail pada struktur sistem fail dapat diakses oleh pengguna atau grup pengguna.

Taktik dan teknik pelaku

Kerangka kerja MITRE ATT&CK adalah kumpulan taktik dan teknik terdokumentasi yang digunakan oleh pelaku ancaman di dunia maya. Kerangka kerja ini dibuat oleh MITRE Corporation, sebuah lembaga nirlaba AS, dan berfungsi sebagai bahasa global umum seputar perilaku pelaku ancaman.

ACSC dari ASD menilai teknik dan taktik berikut relevan dengan aktivitas berbahaya pelaku:

Pengintaian

T1594 – Telusuri Situs Web Milik Korban

Pelaku menelusuri situs web aplikasi web khusus untuk mengidentifikasi peluang mengakses jaringan.

Akses Awal

T1190 – Eksploitasi Aplikasi Public-Facing (mengenai eksploitasi aplikasi web khusus)

T1078.002 – Akun yang Valid: Akun Domain (mengenai logging dengan kredensial yang disusupi)

Eksploitasi aplikasi web khusus yang terekspos internet memberikan titik akses awal bagi pelaku. Pelaku kemudian dapat menggunakan kredensial yang telah disusupi untuk mengakses lebih jauh ke jaringan.

Eksekusi

T1059 – Command dan Scripting Interpreter (mengenai eksekusi perintah melalui web shell)

T1072 – Alat Penerapan Perangkat Lunak (mengenai pelaku yang menggunakan alat sumber terbuka Secure Socket Funnelling (SSF) untuk terhubung ke IP)

Persistensi

T1505.003 – Komponen Perangkat Lunak Server: Web Shell (mengenai penggunaan web shell dan SSF untuk membuat akses)

Akses kredensial

T1552.001 – Kredensial dari Penyimpanan Kata Sandi (mengenai fail kata sandi yang berkaitan dengan building management system (BMS))

T1558.003 – Mencuri atau Memalsukan Tiket Kerberos: Kerberoasting (mengenai serangan untuk mendapatkan kredensial jaringan)

Pergerakan Lateral

T1021.002 – Layanan Jarak Jauh: Berbagi SMB (mengenai pelaku yang memasang berbagi SMB dari beberapa perangkat)

Pengumpulan

T1213 – Data dari Repositori Informasi (mengenai manual/dokumentasi yang ditemukan di server BMS)

Eksfiltrasi

T1041 – Eksfiltrasi Melalui Saluran C2 (mengenai eksfiltrasi data pelaku dari Direktori Aktif dan pemasangan share)

Studi Kasus 2

Laporan ini telah dianonimkan agar dapat disebarluaskan kepada publik. Organisasi yang terdampak selanjutnya disebut sebagai 'organisasi'. Beberapa detail spesifik telah dihapus untuk melindungi identitas korban dan metode respons insiden ACSC ASD.

Ringkasan Eksekutif

Laporan ini memerinci temuan investigasi ACSC ASD atas keberhasilan penyusupan jaringan organisasi pada April 2022. Laporan investigasi ini diberikan kepada organisasi untuk merangkum aktivitas berbahaya yang diamati dan menyusun rekomendasi remediasi. Temuan menunjukkan bahwa pembobolan dilakukan oleh APT40.

Pada bulan Mei 2022, ACSC ASD memberi tahu sebuah organisasi tentang dugaan aktivitas kejahatan yang memengaruhi jaringan organisasi sejak April 2022. Selanjutnya, organisasi tersebut memberi tahu ACSC ASD bahwa mereka telah menemukan perangkat lunak berbahaya di server yang terhubung ke internet yang menyediakan portal masuk untuk solusi akses jarak jauh perusahaan organisasi tersebut. Server ini menggunakan produk manajemen identitas dan login akses jarak jauh dan akan disebut dalam laporan ini sebagai 'perangkat yang disusupi'. Laporan ini memerinci temuan investigasi dan saran remediasi yang dikembangkan untuk organisasi sebagai tanggapan atas investigasi yang dilakukan oleh ACSC ASD.

Bukti menunjukkan bahwa sebagian jaringan organisasi telah disusupi oleh pelaku kejahatan siber melalui portal masuk akses jarak jauh organisasi setidaknya sejak April 2022. Server ini mungkin telah disusupi oleh beberapa pelaku, dan kemungkinan besar terdampak oleh kerentanan eksekusi remote code execution (RCE) yang dipublikasikan secara luas sekitar waktu penyusupan.

Aktivitas pelaku kunci yang diamati oleh ACSC ASD meliputi:

- enumerasi host, yang memungkinkan pelaku untuk membangun peta jaringan mereka sendiri;
- eksploitasi aplikasi yang terhubung ke internet dan penggunaan web shell, yang memberi pelaku pijakan awal di jaringan dan kemampuan untuk melaksanakan perintah;
- eksploitasi kerentanan perangkat lunak untuk meningkatkan hak istimewa; dan
- pengumpulan kredensial untuk memungkinkan pergerakan lateral

ACSC ASD menemukan bahwa pelaku kejahatan telah mengeksfiltrasi beberapa ratus pasangan nama pengguna dan kata sandi unik pada perangkat yang disusupi pada April 2022, serta sejumlah kode autentikasi multifaktor dan artefak teknis yang terkait dengan sesi akses jarak jauh. Setelah ditinjau oleh organisasi, kata sandi tersebut dinyatakan sah. ACSC ASD menilai bahwa pelaku mungkin telah mengumpulkan artefak teknis ini untuk membajak atau membuat sesi login jarak jauh sebagai pengguna yang sah, dan mengakses jaringan internal perusahaan menggunakan akun pengguna yang sah.

Penemuan investigasi

Ringkasan Investigasi

ACSC ASD menetapkan bahwa pelaku telah menyusupi perangkat yang menyediakan sesi login jarak jauh bagi staf organisasi dan menggunakan penyusupan ini untuk mencoba melakukan aktivitas lebih lanjut. Perangkat ini terdiri dari tiga host dengan beban seimbang di mana bukti awal penyusupan terdeteksi. Organisasi menutup dua dari tiga host dengan beban seimbang segera setelah gangguan awal. Akibatnya, semua aktivitas selanjutnya terjadi pada satu host. Server lain yang terkait dengan perangkat yang disusupi juga diseimbangkan bebannya dengan cara yang serupa. Untuk kejelasan, semua perangkat yang disusupi disebut di sebagian besar laporan ini sebagai 'satu perangkat'.

Pelaku diyakini telah menggunakan kerentanan yang diketahui publik untuk menyebarkan web shell ke perangkat yang disusupi mulai April 2022 dan seterusnya. Pelaku ancaman dari kelompok tersebut dinilai telah mencapai hak akses yang ditingkatkan pada perangkat tersebut. ACSC ASD tidak dapat menentukan tingkat aktivitas sepenuhnya karena kurangnya ketersediaan logging. Namun, bukti pada perangkat menunjukkan bahwa seorang pelaku mencapai hal-hal berikut:

- Pengumpulan beberapa ratus pasangan nama pengguna dan kata sandi asli; dan
- Pengumpulan artefak teknis yang mungkin memungkinkan pelaku kejahatan mengakses sesi infrastruktur desktop virtual (VDI) sebagai pengguna yang sah.

ACSC ASD menilai bahwa pelaku tersebut akan berusaha untuk lebih lanjut menyusupi jaringan organisasi. Artefak yang dieksfiltrasi oleh pelaku tersebut mungkin memungkinkan mereka untuk membajak atau memulai sesi desktop virtual sebagai pengguna yang sah, mungkin sebagai pengguna pilihan mereka, termasuk administrator. Pelaku tersebut mungkin telah menggunakan vektor akses ini untuk lebih lanjut menyusupi layanan organisasi guna mencapai persistensi dan tujuan lainnya.

Peralatan organisasi lain dalam lingkungan yang dikelola penyedia hosting tidak menunjukkan bukti penyusupan.

Akses

Host dengan peralatan yang disusupi menyediakan autentikasi melalui Direktori Aktif dan server web, untuk pengguna yang terhubung ke sesi VDI (T1021.001).

Lokasi	Nama host peralatan yang disusupi (load-balanced)
Datacentre 1	HOST1, HOST2, HOST3

Infrastruktur perangkat juga mencakup host gateway akses yang menyediakan terowongan ke VDI bagi pengguna, setelah mereka memiliki token autentikasi yang dibuat dan diunduh dari perangkat.

Tidak ada bukti penyusupan pada host-host ini. Namun, log host gateway akses menunjukkan bukti interaksi signifikan dengan alamat IP berbahaya yang diketahui. Kemungkinan hal ini mencerminkan aktivitas yang terjadi pada host ini, atau koneksi jaringan dengan infrastruktur pelaku ancaman yang mencapai host ini. Sifat aktivitas ini tidak dapat ditentukan menggunakan bukti yang tersedia, tetapi menunjukkan bahwa kelompok tersebut berusaha bergerak secara lateral dalam jaringan organisasi (TA0008).

Host Internal

ACSC ASD menyelidiki data terbatas dari segmen jaringan internal organisasi. Aktivitas berbahaya yang dicoba atau berhasil yang diketahui telah memengaruhi segmen jaringan internal organisasi meliputi akses pelaku ke artefak terkait VDI, pengikisan server SQL internal (T1505.001), dan lalu lintas yang tidak dapat dijelaskan yang teramati berpindah dari alamat IP berbahaya yang diketahui melalui peranti akses gateway (TA0011).

Dengan menggunakan akses mereka ke peranti yang disusupi, kelompok tersebut mengumpulkan nama pengguna, kata sandi (T1003), dan nilai token MFA (T1111) asli. Kelompok tersebut juga mengumpulkan Token Web JSON (JWT) (T1528), yang merupakan artefak autentikasi yang digunakan untuk membuat sesi login desktop virtual. Pelaku tersebut mungkin dapat menggunakan akses ini untuk membuat atau membajak sesi desktop virtual (T1563.002) dan mengakses segmen jaringan internal organisasi sebagai pengguna yang sah (T1078).

Pelaku tersebut juga menggunakan akses ke perangkat yang disusupi untuk mengikis server SQL (T1505.001), yang berada di jaringan internal organisasi. Kemungkinan besar pelaku tersebut memiliki akses ke data ini.

Bukti yang tersedia dari perangkat akses gateway mengungkapkan bahwa lalu lintas jaringan terjadi melalui atau ke perangkat ini dari alamat IP berbahaya yang diketahui. Sebagaimana dijelaskan di atas, hal ini mungkin menunjukkan bahwa pelaku kejahatan siber telah memengaruhi atau memanfaatkan perangkat ini, yang berpotensi untuk beralih ke jaringan internal.

Lini Masa Investigasi

Daftar di bawah ini menyediakan lini masa kegiatan utama yang ditemukan selama investigasi.

Waktu	Peristiwa
April 2022	Alamat IP berbahaya yang diketahui berinteraksi dengan host akses gateway HOST7. Sifat interaksi tidak dapat ditentukan.
April 2022	Semua host, HOST1, HOST2, dan HOST3, telah disusupi oleh satu atau beberapa pelaku kejahatan, dan web shell telah dipasang pada host-host tersebut. Sebuah fail log telah dibuat atau dimodifikasi pada HOST2. Fail ini berisi materi kredensial yang kemungkinan telah dicuri oleh pelaku kejahatan. Fail /etc/security/opasswd dan /etc/shadow telah dimodifikasi pada HOST1 dan HOST3, yang menunjukkan bahwa kata sandi telah diubah. Bukti yang tersedia pada HOST1 menunjukkan bahwa kata sandi untuk pengguna 'sshuser' telah diubah.
April 2022	HOST2 ditutup oleh organisasi. Web shell tambahan (T1505.003) dibuat di HOST1 dan HOST3. HOST1 mengalami upaya brute force SSH dari HOST3. Sebuah fail log dimodifikasi (T1070) di HOST3. Fail ini berisi materi kredensial (T1078) yang kemungkinan besar telah dicuri oleh pelaku kejahatan. JWT telah tertangkap (T1528) dan dikeluarkan ke sebuah fail di HOST3. HOST3 ditutup oleh organisasi. Semua aktivitas setelah periode ini terjadi di HOST1.
April 2022	Web shell tambahan dibuat pada HOST1 (T1505.003). JWT tertangkap dan dikeluarkan menjadi sebuah fail di HOST1.
April 2022	Web shell tambahan dibuat di HOST1 (T1505.003), dan alamat IP berbahaya yang diketahui berinteraksi dengan host (TA0011). Alamat IP berbahaya yang diketahui berinteraksi dengan akses host gateway HOST7.
Mei 2022	Alamat IP berbahaya yang diketahui berinteraksi dengan akses host gateway HOST7 (TA0011). Sebuah peristiwa autentikasi untuk seorang pengguna ditautkan ke alamat IP berbahaya yang diketahui dalam log di HOST1. Sebuah web shell tambahan dibuat pada host ini (T1505.003).
Mei 2022	Sebuah skrip pada HOST1 telah dimodifikasi oleh seorang pelaku (T1543). Skrip ini berisi fungsionalitas yang akan mengambil data dari server SQL internal.
Mei 2022	Fail log tambahan pada HOST1 terakhir dimodifikasi (T1070). Fail ini berisi pasangan nama pengguna dan kata sandi untuk jaringan organisasi, yang diyakini sah (T1078).
Mei 2022	Fail log tambahan terakhir dimodifikasi (T1070). Fail ini berisi JWT yang dikumpulkan dari HOST1.
Mei 2022	Web shell tambahan dibuat pada HOST1 (T1505.003). Pada tanggal ini, organisasi melaporkan penemuan web shell dengan tanggal pembuatan pada bulan April 2022 kepada ACSC ASD.
Mei 2022	Sejumlah skrip dibuat pada HOST1, termasuk satu yang bernama Log4jHotPatch.jar.
Mei 2022	Perintah iptables-save digunakan untuk menambahkan dua porta terbuka ke akses gateway host. Porta tersebut adalah 9998 dan 9999 (T1572).

Taktik dan teknik pelaku

Hal yand disorot berikut ini adalah beberapa taktik dan teknik yang diidentifikasi selama investigasi.

Akses Awal

T1190 Eksploitasi aplikasi public-facing

Kelompok ini kemungkinan besar mengeksploitasi kerentanan RCE, eskalasi hak istimewa, dan bypass autentikasi pada produk manajemen identitas dan login akses jarak jauh untuk mendapatkan akses awal ke jaringan.

Metode akses awal ini dianggap paling mungkin karena hal-hal berikut:

- Server rentan terhadap CVE ini pada saat itu;
- Upaya untuk mengeksploitasi kerentanan ini dari infrastruktur pelaku yang dikenal; dan
- Aktivitas berbahaya internal pertama yang diketahui terjadi tak lama setelah upaya eksploitasi dilakukan.

Eksekusi

T1059.004 Command dan Scripting Interpreter: Unix Shell

Kelompok yang berhasil mengeksploitasi kerentanan di atas mungkin dapat menjalankan perintah di Unix shell yang tersedia pada perangkat yang terdampak. Detail lengkap perintah yang dijalankan oleh pelaku tidak dapat diberikan karena tidak dicatat oleh perangkat.

Persistensi

T1505.003 Komponen Perangkat Lunak Server: Web Shell

Pelaku menyebarkan beberapa web shell pada perangkat yang terdampak. Ada kemungkinan beberapa pelaku yang berbeda menyebarkan web shell, tetapi hanya sedikit pelaku yang melakukan aktivitas menggunakan web shell tersebut. Web shell memungkinkan pelaku untuk mengeksekusi perintah secara sembarangan pada perangkat yang terdampak.

Eskalasi Hak Istimewa

T1068 Eksploitasi untuk Eskalasi Hak Istimewa

Bukti yang tersedia tidak menjelaskan tingkat hak istimewa yang dicapai oleh para pelaku. Namun, dengan menggunakan web shell, para pelaku akan mencapai tingkat hak istimewa yang sebanding dengan server web pada perangkat yang disusupi. Kerentanan yang diyakini terdapat pada perangkat yang disusupi akan memungkinkan para pelaku untuk mendapatkan hak istimewa root.

Akses kredensial

T1056.003 Input Capture: Web Portal Capture

Bukti pada perangkat yang disusupi menunjukkan bahwa pelaku telah mengambil beberapa ratus pasangan nama pengguna dan kata sandi, dalam bentuk teks biasa, yang diyakini sah. Kemungkinan besar pengambilan ini dilakukan dengan menggunakan beberapa modifikasi pada proses autentikasi asli yang menghasilkan kredensial ke sebuah fail.

T1111 Intersepsi Autentikasi Multifaktor

Pelaku juga mengambil nilai token MFA yang sesuai dengan login yang sah. Nilai-nilai ini kemungkinan diambil dengan memodifikasi proses autentikasi asli untuk menghasilkan nilai-nilai ini ke sebuah fail. Tidak ada bukti adanya penyusupan pada 'server rahasia' yang menyimpan nilai-nilai unik yang menjamin keamanan token MFA.

T1040 Network Sniffing

Pelaku diyakini telah mengambil JWT dengan mengambil lalu lintas HTTP pada perangkat yang disusupi. Terdapat bukti bahwa utilitas tcpdump dijalankan pada perangkat yang disusupi, yang mungkin menjadi cara pelaku menangkap JWT ini.

T1539 Mencuri Kuki Sesi Web

Sebagaimana dijelaskan di atas, pelaku menangkap JWT, yang serupa dengan kuki sesi web. Kuki ini dapat digunakan kembali oleh pelaku untuk mendapatkan akses lebih lanjut.

Penemuan

T1046 Penemuan Layanan Jaringan

Terdapat bukti bahwa utilitas pemindaian jaringan nmap dijalankan pada perangkat yang disusupi untuk memindai perangkat lain di segmen jaringan yang sama. Hal ini kemungkinan digunakan oleh pelaku untuk menemukan layanan jaringan lain yang dapat dijangkau yang mungkin memberikan peluang untuk pergerakan lateral.

Pengumpulan

Bukti yang tersedia tidak mengungkapkan bagaimana pelaku mengumpulkan data atau apa tepatnya yang dikumpulkan dari perangkat yang disusupi atau dari sistem lain. Namun, kemungkinan besar pelaku memiliki akses ke semua fail pada perangkat yang disusupi, termasuk kredensial yang dicuri (T1003), nilai token MFA (T1111), dan JWT yang dijelaskan di atas.

Perintah dan kontrol

T1071.001 Protokol Lapisan Aplikasi: Protokol Web

Pelaku menggunakan web shell untuk perintah dan kontrol. Perintah web shell akan diteruskan melalui HTTPS menggunakan server web yang ada di perangkat (T1572).

T1001.003 Pengaburan Data: Impersonasi Protokol

Pelaku menggunakan perangkat yang telah disusupi sebagai titik awal serangan yang dirancang untuk berbaur dengan lalu lintas yang sah.

Rekomendasi Deteksi Dan Mitigasi

ACSC ASD sangat menyarankan penerapan Delapan Kontrol Esensial ASD dan Strategi untuk Memitigasi Insiden Keamanan Siber terkait. Berikut adalah rekomendasi tindakan keamanan jaringan yang harus diambil untuk mendeteksi dan mencegah intrusi oleh APT40, diikuti dengan mitigasi spesifik untuk empat TTP utama yang dirangkum dalam Tabel 1.

Deteksi

Beberapa fail yang diidentifikasi disisipkan di lokasi seperti C:\Users\Public* dan C:\Windows\Temp*. Lokasi-lokasi ini dapat menjadi tempat yang nyaman untuk menulis data karena biasanya dapat ditulis oleh semua orang, artinya, semua akun pengguna yang terdaftar di Windows memiliki akses ke direktori ini dan subdirektorinya. Seringkali, setiap pengguna selanjutnya dapat mengakses fail-fail ini, yang memungkinkan terjadinya pergerakan lateral, penghindaran pertahanan, eksekusi dengan hak istimewa rendah, dan persiapan untuk eksfiltrasi.

Aturan Sigma berikut mencari eksekusi dari lokasi yang mencurigakan sebagai indikator aktivitas anomali. Dalam semua kasus, investigasi lanjutan diperlukan untuk mengonfirmasi aktivitas berbahaya dan atribusinya.

Judul: Eksekusi yang Dapat Dilakukan Semua Orang - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Deskripsi: Deteksi eksekusi proses dari C:\Windows\Temp.

Latar Belakang:

Aturan ini secara khusus mencari eksekusi dari C:\Windows\Temp*. Temp lebih umum digunakan oleh aplikasi jinak sehingga merupakan indikator berbahaya dengan tingkat keyakinan yang lebih rendah dibandingkan eksekusi dari subdirektori lain yang dapat ditulis semua orang di C:\Windows.

Menghapus aplikasi yang dijalankan oleh pengguna SYSTEM atau NETWORK SERVICE secara substansial mengurangi jumlah aktivitas jinak yang dipilih oleh aturan ini.

Ini berarti aturan ini mungkin melewatkan eksekusi berbahaya pada tingkat hak istimewa yang lebih tinggi, tetapi disarankan untuk menggunakan aturan lain guna menentukan apakah pengguna mencoba meningkatkan hak istimewa ke SYSTEM.

Investigasi:

1. Periksa informasi yang terkait langsung dengan eksekusi fail ini, seperti konteks pengguna, tingkat integritas eksekusi, aktivitas lanjutan langsung, dan gambar yang dimuat oleh fail.
2. Selidiki proses kontekstual, jaringan, fail, dan data pendukung lainnya pada host untuk membantu menilai apakah aktivitas tersebut berbahaya.
3. Jika perlu, cobalah mengumpulkan salinan fail untuk direkayasa balik guna menentukan keabsahannya.

Referensi:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Penulis: ACSC ASD

Tanggal: 19-06-2024

Status: eksperimental

Tag:

- tlp.green
- classification.au.official
- attack.execution

Sumber Log:

kategori: process_creation
produk: windows

Deteksi:

```
temp:
    Image|startswith: 'C:\\Windows\\Temp\\'
common_temp_path:
    Image|re|ignorecase: 'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user:
    User:
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

kondisi: sementara dan bukan (common_temp_path atau system_user atau dismhost atau known_parent)

Positif palsu:

- Aplikasi audit daftar putih telah diamati menjalankan fail yang dapat dieksekusi dari Temp.
- Temp seharusnya berisi serangkaian aplikasi pengaturan dan peluncur, jadi ada baiknya mempertimbangkan seberapa umum perilaku ini di jaringan yang dipantau (dan apakah dapat dimasukkan ke daftar putih atau tidak) sebelum menerapkan aturan ini.

Tingkat: rendah

Judul: Eksekusi Subdirektori Sistem - Non-Temp yang Dapat Ditulis Oleh Semua Orang

ID: 5b187157-e892-4fc9-84fc-aa48aff9f997

Deskripsi: Mendeteksi eksekusi proses dari lokasi yang dapat ditulis semua orang di subdirektori lokasi instalasi OS Windows.

Latar Belakang:

Aturan ini secara khusus mencari eksekusi di luar direktori yang dapat ditulis oleh semua orang dalam C:\ dan khususnya C:\Windows*, dengan pengecualian C:\Windows\Temp (yang lebih luas digunakan oleh aplikasi jinak dan dengan demikian merupakan indikator berbahaya dengan tingkat keyakinan yang lebih rendah).

Folder AppData dikecualikan jika suatu fail dijalankan sebagai SYSTEM - ini adalah cara yang jinak untuk mengeksekusi banyak fail aplikasi sementara.

Setelah menyelesaikan dasar jaringan awal dan mengidentifikasi eksekusi yang diketahui jinak dari lokasi-lokasi ini, aturan ini seharusnya jarang dijalankan.

Investigasi:

1. Periksa informasi yang terkait langsung dengan eksekusi fail ini, seperti konteks pengguna, tingkat integritas eksekusi, aktivitas lanjutan langsung, dan gambar yang dimuat oleh fail.
2. Selidiki proses kontekstual, jaringan, fail, dan data pendukung lainnya pada host untuk membantu menilai apakah aktivitas tersebut berbahaya.
3. Jika perlu, cobalah untuk mengumpulkan salinan fail untuk direkayasa balik guna menentukan keabsahannya.

Referensi:

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Penulis: ACSC ASD

Tanggal: 19-06-2024

Status: eksperimental

Tag:

- tlp.green
- classification.au.official
- attack.execution

Sumber log:

kategori: process_creation

produk: windows

Deteksi:

writable_path:

Image|contains:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'

- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Image|contains: '\\AppData\\'
User: 'SYSTEM'

kondisi: writable_path dan bukan appdata

Positif palsu:

Aplikasi audit daftar putih telah diamati menjalankan eksekusi dari direktori ini.

Masuk akal jika skrip dan alat administratif yang digunakan dalam lingkungan yang dipantau mungkin terletak di salah satu direktori ini dan harus ditangani berdasarkan kasus per kasus.

Tingkat: tinggi

Judul: Eksekusi yang Dapat Dilakukan Semua Orang - Users

ID: 6dda3843-182a-4214-9263-925a80b4c634

Deskripsi: Mendeteksi eksekusi proses dari C:\Users\Public* dan folder lain yang dapat ditulis oleh semua orang di dalam Users.

Latar Belakang:

Folder AppData dikecualikan jika suatu fail dijalankan sebagai SYSTEM - ini adalah cara yang jinak untuk mengeksekusi banyak fail aplikasi sementara.

Investigasi:

1. Periksa informasi yang terkait langsung dengan eksekusi fail ini, seperti konteks pengguna, tingkat integritas eksekusi, aktivitas lanjutan langsung, dan gambar yang dimuat oleh fail.
2. Selidiki proses kontekstual, jaringan, fail, dan data pendukung lainnya pada host untuk membantu menilai apakah aktivitas tersebut berbahaya.
3. Jika perlu, cobalah mengumpulkan salinan fail untuk direkayasa balik guna menentukan keabsahannya.

Referensi:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

Penulis: ACSC ASD

Tanggal: 19-06-2024

Status: eksperimental

Tag:

- tlp.green
- classification.au.official
- attack.execution

Sumber log:

kategori: process_creation
produk: windows

Deteksi:

users:

Image|contains:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:

Image|contains: '\\AppData\\'

User: 'SYSTEM'

kondisi: pengguna dan bukan appdata

Positif palsu:

- Masuk akal jika skrip dan alat administratif yang digunakan dalam lingkungan yang dipantau mungkin berlokasi di Publik atau subdirektori dan harus ditangani berdasarkan kasus per kasus.

Tingkat: medium

Mitigasi

Logging

Selama investigasi ACSC ASD, masalah umum yang mengurangi efektivitas dan kecepatan upaya investigasi adalah kurangnya informasi logging yang komprehensif dan historis di sejumlah area, termasuk log permintaan server web, log peristiwa Windows, dan log proksi internet.

ACSC ASD menyarankan untuk meninjau dan menerapkan panduan mereka tentang Logging dan Forwarding Windows Event termasuk fail konfigurasi dan skrip dalam Windows Event Logging Repository dan Pedoman Pemantauan Sistem dari Manual Keamanan Informasi, untuk mencakup pemusatan log dan penyimpanan log untuk periode yang sesuai.

Manajemen patch

Segera patch semua perangkat dan layanan yang terpapar internet, termasuk server web, aplikasi web, dan akses gateway jarak jauh. Pertimbangkan untuk menerapkan sistem manajemen patch terpusat untuk mengotomatiskan dan mempercepat proses. ACSC ASD merekomendasikan penerapan Pedoman Manajemen Sistem ISM, khususnya, kontrol System Patching jika berlaku.

Sebagian besar eksploitasi yang digunakan oleh pelaku kejahatan siber telah diketahui publik dan memiliki patch atau mitigasi yang tersedia. Organisasi harus memastikan bahwa patch atau mitigasi keamanan diterapkan ke infrastruktur yang terhubung ke internet dalam waktu 48 jam, dan jika memungkinkan, gunakan versi perangkat lunak dan sistem operasi terbaru.

Segmentasi jaringan

Segmentasi jaringan dapat mempersulit penyerang untuk menemukan dan mendapatkan akses ke data sensitif suatu organisasi secara signifikan. Segmentasi jaringan untuk membatasi atau memblokir pergerakan lateral dengan menolak lalu lintas antar komputer kecuali diperlukan. Server penting seperti Active Directory dan server autentikasi lainnya seharusnya hanya dapat dikelola dari sejumlah server perantara atau 'jump server' yang terbatas. Server-server ini harus dipantau secara ketat, diamankan dengan baik, dan dibatasi pengguna serta perangkat mana yang dapat terhubung.

Terlepas dari kasus-kasus yang teridentifikasi di mana pergerakan lateral dicegah, segmentasi jaringan tambahan dapat semakin membatasi jumlah data yang dapat diakses dan diekstraksi oleh para pelaku.

Mitigasi tambahan

Badan penyusun juga merekomendasikan mitigasi berikut untuk mencegah penggunaan TTP oleh APT40 dan pihak lain di bawah ini.

- Nonaktifkan layanan jaringan, porta, dan protokol yang tidak digunakan atau tidak diperlukan.
- Gunakan Web application firewalls (WAF) yang disetel dengan baik untuk melindungi server web dan aplikasi.
- Terapkan hak istimewa terkecil untuk membatasi akses ke server, berbagi fail, dan sumber daya lainnya.
- Gunakan multi-factor authentication (MFA) dan akun layanan terkelola untuk mempersulit penyusupan dan penggunaan kembali kredensial. MFA harus diterapkan ke semua layanan akses jarak jauh yang dapat diakses melalui internet, termasuk:
  - Sur-el berbasis web dan cloud
  - Platform kolaborasi
  - Koneksi virtual private network (VPN)
  - Layanan desktop jarak jauh
- Ganti peralatan yang sudah habis masa pakainya.

Tabel 1. Strategi/Teknik Mitigasi

TTP	Delapan Strategi Mitigasi Penting	Kontrol ISM
Akses Awal T1190 Eksploitasi Aplikasi Public-Facing	Aplikasi patch Sistem operasi patch Autentikasi Multifaktor Kontrol aplikasi	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Eksekusi T1059 Command dan Scripting Interpreter	Kontrol aplikasi Batasi makro Microsoft Office Batasi hak akses administratif	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Persistensi T1505.003 Komponen Perangkat Lunak Server: Web Shell	Kontrol Aplikasi Batasi hak akses administratif	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Akses Awal/Eskalasi Hak Istimewa/Persistensi T1078 Akun yang Valid	Sistem operasi patch Autentikasi Multifaktor Batasi hak akses administratif Kontrol aplikasi Pengerasan aplikasi pengguna	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

Untuk saran deteksi dan mitigasi umum tambahan, silakan lihat bagian Mitigasi dan Deteksi di halaman web teknik MITRE ATT&CK untuk setiap teknik yang diidentifikasi dalam ringkasan MITRE ATT&CK di akhir saran ini.

Penafian

Informasi dalam laporan ini disediakan "sebagaimana adanya" untuk tujuan yang bersifat informasi saja. Badan penyusun tidak mendukung entitas komersial, produk, perusahaan, atau layanan apa pun, termasuk entitas, produk, atau layanan apa pun yang tertaut dalam dokumen ini. Segala rujukan ke entitas komersial, produk, proses, atau layanan tertentu melalui merek layanan, merek dagang, produsen, atau lainnya, tidak merupakan atau menyiratkan dukungan, rekomendasi, atau dukungan dari badan penyusun.

Dokumen ini ditandai TLP:CLEAR. Pengungkapan tidak terbatas. Sumber dapat menggunakan TLP:CLEAR ketika informasi tersebut memiliki risiko penyalahgunaan yang minimal atau tidak ada, sesuai dengan aturan dan prosedur yang berlaku untuk rilis publik. Sesuai dengan aturan hak cipta standar, informasi TLP:CLEAR dapat didistribusikan tanpa batasan. Untuk informasi lebih lanjut tentang Protokol Lampu Lalu Lintas, kunjungi cisa.gov/tlp

MITRE ATT&CK – Sejarah kemahiran spionase APT40 yang Dimaksud

Pengintaian (TA0043)	
Telusuri Situs Web Milik Korban (T1594)	Kumpulkan Informasi Identitas Korban: Kredensial (T1589.001)
Pemindaian Aktif: Pemindaian Kerentanan (T1595.002)	Kumpulkan Informasi Host Korban (T1592)
Mencari Situs Web/Domain Terbuka: Mesin Pencari (T1593.002)	Kumpulkan Informasi Jaringan Korban: Properti Domain (T1590.001)
Kumpulkan Informasi Identitas Korban: Alamat Sur-el (T1589.002)	

Pengembangan Sumber Daya (TA0042)	
Peroleh Infrastruktur: Domain (T1583.001)	Peroleh Infrastruktur (T1583)
Peroleh Infrastruktur: Server DNS (T1583.002)	Susupi Akun (T1586)
Kembangkan Kemampuan: Sertifikat Penandatanganan Kode (T1587.002)	Susupi Infrastruktur (T1584)
Kembangkan Kemampuan: Sertifikat Digital (T1587.003)	Kembangkan Kemampuan: Malware (T1587.001)
Peroleh Kemampuan: Sertifikat Penandatanganan Kode (T1588.003)	Buat Akun: Akun Cloud (T1585.003)
Susupi Infrastruktur: Perangkat Jaringan (T1584.008)	Peroleh Kemampuan: Sertifikat Digital (T1588.004)

Akses Awal (TA0001)	
Akun yang Valid (T1078)	Phishing (T1566)
Akun yang Valid: Akun Asal (T1078.001)	Phishing: Lampiran Spearphishing (T1566.001)
Akun yang Valid: Akun Domain (T1078.002)	Phishing: Tautan Spearphishing (T1566.002)
Layanan Jarak Jauh Eksternal (T1133)	Eksploitasi Aplikasi Public-Facing (T1190)
Penyusupan Drive-by (T1189)	

Eksekusi (TA0002)	
Instrumentasi Manajemen Windows (T1047)	Command dan Scripting Interpreter: Python (T1059.006)
Tugas/Pekerjaan Terjadwal: At (T1053.002)	Command dan Scripting Interpreter: JavaScript (T1059.007)
Tugas/Pekerjaan Terjadwal: Tugas Terjadwal (T1053.005)	API Asli (T1106)
Command dan Scripting Interpreter (T1059)	Komunikasi Antarproses (T1559)
Command dan Scripting Interpreter: Windows Command Shell (T1059.003)	Layanan Sistem: Eksekusi Layanan (T1569.002)
Command dan Scripting Interpreter: PowerShell (T1059.001)	Eksploitasi untuk Eksekusi Klien (T1203)
Command dan Scripting Interpreter: Visual Basic (T1059.005)	Eksekusi User: Fail Berbahaya (T1204.002)
Command dan Scripting Interpreter: Unix Shell (T1059.004)	Command dan Scripting Interpreter: Apple Script (T1059.002)
Tugas/Pekerjaan Terjadwal: Cron (T1053.003)	Alat Penyebaran Perangkat Lunak (T1072)

Persistensi (TA0003)	
Akun yang Valid (T1078)	Komponen Perangkat Lunak Server: Web Shell (T1505.003)
Startup Aplikasi Office: Office Template Macros (T1137.001)	Buat atau Modifikasi Proses Sistem: Windows Service (T1543.003)
Tugas/Pekerjaan Terjadwal: At (T1053.002)	Boot or Logon Autostart Execution: Kunci Run Registri/ Folder Startup (T1547.001)
Tugas/Pekerjaan Terjadwal: Tugas Terjadwal (T1053.005)	Boot or Logon Autostart Execution: Modifikasi Pintasan (T1547.009)
Layanan Jarak Jauh Eksternal (T1133)	Alur Eksekusi Pembajakan: DLL Search Order Hijacking (T1574.001)
Tugas/Pekerjaan Terjadwal: Cron (T1053.003)	Alur Eksekusi Pembajakan: DLL Side-Loading (T1574.002)
Manipulasi Akun (T1098)	Akun yang Valid: Akun Cloud (T1078.004)
Akun yang Valid: Akun Domain (T1078.002)	

Eskalasi Hak Istimewa (TA0004)	
Tugas/Pekerjaan Terjadwal: At (T1053.002)	Buat atau Modifikasi Proses Sistem: Windows Service (T1543.003)
Tugas/Pekerjaan Terjadwal: Tugas Terjadwal (T1053.005)	Boot or Logon Autostart Execution: Kunci Run Registri/ Folder Startup (T1547.001)
Injeksi Proses: Pembajakan Eksekusi Thread (T1055.003)	Boot or Logon Autostart Execution: Modifikasi Pintasan (T1547.009)
Injeksi Proses: Pengosongan Proses (T1055.012)	Alur Eksekusi Pembajakan: DLL Search Order Hijacking (T1574.001)

Eskalasi Hak Istimewa (TA0004)	
Akun yang Valid: Akun Domain (T1078.002)	Eksploitasi untuk Eskalasi Hak Istimewa (T1068)
Manipulasi Token Akses: Peniruan/Pencurian Token (T1134.001)	Eksekusi yang Dipicu Peristiwa: Modifikasi Konfigurasi Shell Unix (T1546.004)
Injeksi Proses: Injeksi Pustaka Tautan Dinamis (T1055.001)	Akun yang Valid: Akun Domain (T1078.002)
Akun yang Valid: Akun Lokal (T1078.003)	

Penghindaran Pertahanan (TA0005)	
Rootkit (T1014)	Eksekusi Perintah Tidak Langsung (T1202)
Fail atau Informasi yang Dikaburkan (T1027)	Eksekusi Proksi Biner Sistem: Mshta (T1218.005)
Fail atau Informasi yang Dikaburkan: Pengemasan Perangkat Lunak (T1027.002)	Eksekusi Proksi Biner Sistem: Regsvr32 (T1218.010)
Fail atau Informasi yang Dikaburkan: Steganografi (T1027.003)	Mengubah Kontrol Kepercayaan: Penandatanganan Kode (T1553.002)
Fail atau Informasi yang Dikaburkan: Kompilasi Setelah Pengiriman (T1027.004)	Modifikasi Izin Fail dan Direktori: Modifikasi Izin Fail dan Direktori Linux dan Mac (T1222.002)
Penyamaran: Cocokkan Nama atau Lokasi yang Sah (T1036.005)	Virtualisasi/Penghindaran Sandbox: Pemeriksaan Sistem (T1497.001)
Injeksi Proses: Pembajakan Eksekusi Thread (T1055.003)	Penyamaran (T1036)
Pemuatan Kode Reflektif (T1620)	Merusak Pertahanan: Nonaktifkan atau Ubah Firewall Sistem (T1562.004)
Injeksi Proses: Pengosongan Proses (T1055.012)	Sembunyikan Artefak: Fail dan Direktori Tersembunyi (T1564.001)
Penghapusan Indikator: Penghapusan Fail (T1070.004)	Sembunyikan Artefak: Jendela Tersembunyi (T1564.003)
Penghapusan Indikator: Timestomp (T1070.006)	Alur Eksekusi Pembajakan: DLL Search Order Hijacking (T1574.001)
Penghapusan Indikator: Hapus Log Peristiwa Windows (T1070.001)	Alur Eksekusi Pembajakan: DLL Side-Loading (T1574.002)
Ubah Registri (T1112)	Layanan Web (T1102)
Deobfuscate/Decode Fail atau Informasi (T1140)	Penyamaran: Tugas atau Layanan Penyamaran (T1036.004)
Merusak Pertahanan (T1562)	

Akses Kredensial (TA0006)	
OS Credential Dumping: Memori LSASS (T1003.001)	Kredensial Tidak Aman: Kredensial dalam Fail (T1552.001)
OS Credential Dumping: NTDS (T1003.003)	Brute Force: Tebak Kata Sandi (T1110.001)
Network Sniffing (T1040)	Autentikasi Paksa (T1187)

Akses Kredensial (TA0006)	
Kredensial dari Penyimpanan Kata Sandi: Keychain (T1555.001)	Mencuri atau Memalsukan Tiket Kerberos: Kerberoasting (T1558.003)
Input Capture: Keylogging (T1056.001)	Intersepsi Autentikasi Multifaktor (T1111)
Mencuri Kuki Sesi Web (T1539)	Mencuri Token Akses Aplikasi (T1528)
Eksploitasi untuk Akses Kredensial (T1212)	Brute Force: Peretasan Kata Sandi (T1110.002)
Input Capture: Pencurian Portal Web (T1056.003)	OS Credential Dumping: DCSync (T1003.006)
Kredensial dari Penyimpanan Kata Sandi (T1555)	Kredensial dari Penyimpanan Kata Sandi: Kredensial dari Peramban Web (T1555.003)

Penemuan (TA0007)	
Penemuan Layanan Sistem (T1007)	Penemuan Informasi Sistem (T1082)
Penemuan Aplikasi Window (T1010)	Penemuan Akun: Akun Lokal (T1087.001)
Registri Kueri (T1012)	Penemuan Informasi Sistem, Teknik T1082 - Enterprise | MITRE ATT&CK®
Penemuan Fail dan Direktori (T1083)	Penemuan Waktu Sistem (T1124)
Penemuan Layanan Jaringan (T1046)	Penemuan Pemilik/Pengguna Sistem (T1033)
Penemuan Sistem Jarak Jauh (T1018)	Penemuan Kepercayaan Domain (T1482)
Penemuan Akun: Akun Sur-el (T1087.003)	Penemuan Akun: Akun Domain (T1087.002)
Penemuan Koneksi Jaringan Sistem (T1049)	Virtualisasi/Penghindaran Sandbox: Pemeriksaan Sistem (T1497.001)
Penemuan Proses (T1057)	Penemuan Perangkat Lunak (T1518)
Penemuan Grup Izin: Grup Domain (T1069.002)	Penemuan Berbagi Jaringan, Teknik T1135 - Enterprise | MITRE ATT&CK®
Penemuan Konfigurasi Jaringan Sistem: Penemuan Koneksi Internet (T1016.001)	

Pergerakan Lateral (TA0008)	
Layanan Jarak Jauh: Protokol Desktop Jarak Jauh (T1021.001)	Layanan Jarak Jauh (T1021)
Layanan Jarak Jauh: Berbagi Admin SMB/Windows (T1021.002)	Gunakan Materi Autentikasi Alternatif: Teruskan Tiket (T1550.003)
Layanan Jarak Jauh: Manajemen Jarak Jauh Windows (T1021.006)	Transfer Alat Lateral (T1570)

Pengumpulan (TA0009)	
Data dari Sistem Lokal (T1005)	Arsipkan Data yang Dikumpulkan: Arsipkan melalui Pustaka (T1560.002)
Data dari Network Shared Drive (T1039)	Pengumpulan Sur-el: Pengumpulan Sur-el Jarak Jauh (T1114.002)

Pengumpulan (TA0009)	
Input Capture: Keylogging (T1056.001)	Clipboard Data (T1115)
Pengumpulan Otomatis (T1119)	Data dari Repositori Informasi (T1213)
Input Capture: Pencurian Portal Web (T1056.003)	Data yang Disusun Bertahap: Remote Data Staging (T1074.002)
Data yang Disusun Bertahap: Local Data Staging (T1074.001)	Arsipkan Data yang Dikumpulkan (T1560)
Pengumpulan Sur-el (T1114)	

Eksfiltrasi (TA0010)	
Eksfiltrasi Melalui Saluran C2 (T1041)	Eksfiltrasi Melalui Protokol Alternatif: Eksfiltrasi Melalui Protokol Non-C2 Asimetris Terenkripsi (T1048.002)
Eksfiltrasi Melalui Protokol Alternatif (T1048)	Eksfiltrasi Melalui Layanan Web: Eksfiltrasi ke Penyimpanan Cloud (T1567.002)

Perintah dan Kontrol (TA0011)	
Pengaburan Data: Impersonasi Protokol (T1001.003)	Layanan Web: Dead Drop Resolver (T1102.001)
Porta yang Umum Digunakan (T1043)	Layanan Web: Komunikasi Satu Arah (T1102.003)
Protokol Lapisan Aplikasi: Protokol Web (T1071.001)	Transfer Alat Ingress (T1105)
Protokol Lapisan Aplikasi: Protokol Transfer Fail (T1071.002)	Proksi: Proksi Internal (T1090.001)
Proksi: Proksi Eksternal (T1090.002)	Porta Non-Standar (T1571)
Proksi: Proksi Multi-hop (T1090.003)	Penerowongan Protokol (T1572)
Layanan Web: Komunikasi Dua Arah (T1102.002)	Saluran Terenkripsi (T1573)
Saluran Terenkripsi: Kriptografi Asimetris (T1573.002)	Transfer Alat Ingress (T1105)
Proksi, Teknik T1090 - Enterprise | MITRE ATT&CK®	

Dampak (TA0040)	
Penghentian Layanan (T1489)	Disk Wipe (T1561)
Shutdown/Reboot Sistem (T1529)	Pembajakan Sumber Daya (T1496)

Catatan

Penafian

Materi dalam panduan ini bersifat umum dan tidak boleh dianggap sebagai nasihat hukum atau diandalkan untuk bantuan dalam keadaan tertentu atau situasi darurat. Dalam masalah penting apa pun, Anda harus mencari nasihat profesional independen yang sesuai sehubungan dengan keadaan Anda sendiri.

Persemakmuran tidak bertanggung jawab atau berkewajiban atas kerusakan, kerugian, atau biaya apa pun yang ditimbulkan sebagai akibat mengandalkan informasi yang terkandung dalam panduan ini.

Hak Cipta

Penggunaan lambang Coat of Arms

Persyaratan penggunaan Lambang Coat of Arms diperinci di situs web Department of the Prime Minister and Cabinet Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

Untuk informasi lebih lanjut, atau untuk melaporkan insiden keamanan siber, hubungi kami:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Nomor ini hanya dapat digunakan di Australia.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre